ROPES & GRAY ALERT

Health Care ▪ Digital Health

February 19, 2016

# Health Apps and HIPAA: OCR Publishes New Privacy Guidance for Health App Developers

On February 11, 2016, in response to requests from developers of mobile health applications, the Department of Health and Human Services Office for Civil Rights ("OCR") released a new guidance document addressing the applicability of the Health Insurance Portability and Accountability Act ("HIPAA") to applications that collect, store or transmit health information. The guidance document, entitled "Health App Use Scenarios & HIPAA" ("Health App Guidance"), sets forth several factual scenarios involving mobile health apps, along with OCR's explanation of whether, in each scenario, HIPAA would apply to the developer of the app.

## Highlights

- OCR's Health App Guidance details six scenarios in which Health Apps collect, store and/or transmit health information directly from consumers and analyzes the relationships developers may have with: (i) consumers/patients, (ii) covered entities ("CEs"), *i.e.*, those entities that are governed directly by HIPAA (health care providers, health plans and clearinghouses) and (iii) business associates ("BAs"), *i.e.*, persons or entities that receive protected health information ("PHI") in order to perform certain functions or activities on behalf of CEs.
- The Health App Guidance also clarifies that a health app that is downloaded and used solely by individual consumers does not result in the app developer's becoming subject to HIPAA. The reason for this result is that the developer is not creating, receiving, maintaining or transmitting PHI on behalf of a CE or BA. On the contrary, the PHI being used or stored by the app is directly from, and for, the consumer.
- However, a developer who contracts directly with a CE to collect, maintain or transmit PHI through a particular health app is deemed to be a BA under HIPAA, and accordingly will be subject to HIPAA requirements because the developer is providing a service for the benefit of the CE and has access to the PHI of the CE. A developer who contracts with a BA on behalf of a CE to do the same thing likewise will be subject to HIPAA.

## Major Elements of OCR Health App Guidance

The Health App Guidance is the latest development to arise from OCR's mHealth Developer Portal, a platform launched last fall that allows health app developers and others to ask OCR questions regarding health technology and privacy laws, including HIPAA. The mHealth Developer Portal also serves as a vehicle for OCR to publish guidance to educate developers on how HIPAA regulations may apply to new technologies.

The Health App Guidance describes, through the use of six specific scenarios, a broad spectrum of health apps. Health apps that are created and offered directly by or on behalf of CEs or BAs and that store or transmit PHI unambiguously are subject to HIPAA. For example, an independent health app developer that contracts with a health care provider ("Provider") and creates a health app that allows patients to access and manage their health records as part of the Provider's patient portal is clearly a BA and, therefore, must follow all requirements of HIPAA and related regulations.

**Scenarios in which Health Apps are Not BAs.** The Health App Guidance provides additional clarity for developers who create health apps that are downloaded and used solely by individual consumers. The individual consumer is not

a CE or a BA and is voluntarily downloading the app for his/her personal use. Therefore, these developers are not creating, receiving, maintaining or transmitting PHI on behalf of a CE or BA. Accordingly, OCR has stated that such a developer is clearly not a BA for this same reason even if: (i) a Provider recommends the health app to his or her patient, (ii) the consumer uploads his or her electronic health record ("EHR") to the health app from a Provider's patient portal or (iii) the app developer enters into an interoperability agreement with the Provider that allows the consumer to transmit information from the health app to the Provider.

**Scenarios in which Health Apps are BAs.** In contrast, the Health App Guidance details two scenarios in which a developer will be classified as a BA. In the first scenario, a Provider has contracted directly with the health app developer for patient management services, services that include remote patient health counseling, monitoring of patients' food and exercise, patient messaging and EHR integration. In the second scenario, a health plan ("Plan") offers a health app that allows Plan members to download and store health plan records, to check the status of claims/coverage decisions and to document and track their general wellness information. The Plan then analyzes the health and wellness information uploaded to the health app by members. Because both the Provider and the Plan as CEs are contracting directly with the Health App developer it is considered a BA. In contrast, in this latter scenario, the Health App Guidance specifies that if the same developer offers a separate, direct-to-consumer version of the health app with the same functionality, this version of the health app would not be subject to the HIPAA rules as long as the developer keeps the health information contained in the two versions of the health app entirely separate.

**OCR's Key Questions.** The Health App Guidance concludes with a series of questions that developers should consider about their business and their health apps to determine if they are BAs. These questions include: (i) whether the health app creates, receives, maintains or transmits identifiable information; (ii) who the clients for the health app are, and whether those clients include CEs or BAs; (iii) whether the health app is selected independently by the consumer; (iv) whether all decisions to transmit health data to third parties are controlled by the consumer; and (v) whether the developer has any contractual or other relationships with third party entities, other than interoperability agreements. OCR does not provide an analysis of exactly how the answers to these questions may affect classification of a health app developer as a BA; instead, and key to the analysis, OCR offers these questions to help developers determine whether their health app's functions and business model focus primarily on consumers, or on creating, receiving, maintaining or transmitting PHI for CEs. If the health app is focused on the latter, its developer will be classified as a BA and be subject to HIPAA.

## Context of OCR Health App Guidance

The Health App Guidance follows requests from app developers for additional guidance from OCR on when and how HIPAA applies to the burgeoning field of health apps. OCR has signaled its intention that the Health App Guidance will provide needed clarity and facilitate innovation. Jocelyn Samuels, the Director of OCR, has written in a blog post: "We hope these new scenarios will help developers determine how federal regulations might apply to products they are building; we also hope they will reduce some of the uncertainty that can be a barrier to innovation."

If you have any questions about this guidance document or about how HIPAA may apply to health applications, please contact your usual Ropes & Gray attorney.